

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS

Jimmy Tuan Tran

Plaintiff,

vs.

Civil Action No. 4:24-cv-04769

Defendant “1” a/k/a “Miko” and John Doe Defendants 1-4 who are the cohorts of Defendant “1” and are the owners of the following cryptocurrency deposit wallets where Plaintiff’s stolen cryptocurrency assets were transferred:

Binance:

0x7b338050e5002de4b4963401d73fb4ec507cc812

OKX:

0x71fbc4ba1608bb110ba9ee7725b6869cbf33a2bb

HTX:

0x8552681ca9fdb2be3b383c4fd0e90b3789609253

and

Crypto.com:

0x8c8cf418be7dce2f288486ccc7b3680293376c5f

Defendant(s).

**PLAINTIFF JIMMY TUAN TRAN’S EX PARTE MOTION FOR EXPEDITED
DISCOVERY AND LEAVE TO SERVE THIRD PARTY SUBPOENAS**

COMES NOW, Plaintiff JIMMY TUAN TRAN, by and through undersigned counsel, pursuant to Federal Rules of Civil Procedure 26 and 45 and hereby moves this Court for an Order granting leave to take expedited discovery and to serve third-party subpoenas before the Rule 26(f) Conference. In support of this Motion, Plaintiff states as follows:

I. INTRODUCTION

This case involves the theft of cryptocurrency assets by Defendants whose true identities remain unknown. Defendants used aliases in communications with Plaintiff to shield their true identities and to conceal their fraudulent intent. As part of the Defendants’ fraudulent scheme,

Defendants opened cryptocurrency exchange accounts to launder Plaintiff's stolen assets. To do this, Defendants would have provided identifying information, including copies of their passports or driver's licenses, to the exchanges.

Plaintiff seeks leave to serve third-party subpoenas on the cryptocurrency exchanges to obtain information necessary to identify and serve the Defendants. The respective cryptocurrency exchanges have either not responded to Plaintiff's requests or have informed Plaintiff a subpoena would be necessary to produce any account information. Furthermore, expedited discovery is necessary to prevent further dissipation of assets and to allow this case to proceed.

II. BACKGROUND

As set forth in Plaintiff's Complaint, Defendants stole 5,136 USDT, 140.05 ETH, and 172,043 USDC from Plaintiff, which at the time of filing Plaintiff's complaint had a market value of approximately six hundred and sixty-two thousand eight hundred and fifty five dollars and sixty cents. Compl. at ¶ 1.

Defendants are as yet unidentified individuals, business entities and/or unincorporated associations and companies operating a sophisticated global internet cryptocurrency fraud and conversion scheme. Defendants used electronic means of communication and used the blockchain to convert cryptocurrency from victims, including and specifically Plaintiff, in the United States. Plaintiff has tracked his stolen cryptocurrency to Defendants' Crypto Wallets.

Defendants have maintained, and continue to maintain, private cryptocurrency wallets and cryptocurrency exchange accounts ("Defendants' Crypto Wallets") in which all or a portion of Plaintiff's stolen cryptocurrency currently sits. *Id.* at ¶ 13.

Plaintiff has retained forensic cryptocurrency tracing experts who have traced Plaintiff's stolen assets on the blockchain. *Id.* at 40. Plaintiff tracked the stolen cryptocurrency to the

identified electronic wallets at four (4) exchanges: Binance, OKX, HTX, and Crypto.com. *See* Exhibit A to Compl. at 13.

Defendants provided Plaintiff with fraudulent information about their true identities. Plaintiff has attempted through multiple informal requests to obtain information regarding the identities and physical addresses of Defendants from the exchanges where Defendants' cryptocurrency wallets are located to no avail.

Defendants' scheme bears the unmistakable characteristics of a Southeast Asian pig-butcher scam. In September of 2023, FinCEN issued an alert to warn United States citizens of the threat of pig butchering scam, explaining:

“Pig butchering” scams resemble the practice of fattening a hog before slaughter. Victims invest in supposedly legitimate virtual currency investment opportunities before they are conned out of their money. Scammers refer to victims as “pigs,” and may leverage fictitious identities, the guise of potential relationships, and elaborate storylines to “fatten up” the victim into believing they are in trusted partnerships before they defraud the victims of their assets—the “butchering.” These scams are largely perpetrated by criminal enterprises based in Southeast Asia who use victims of labor trafficking to conduct outreach to millions of unsuspecting individuals around the world.¹

Likewise, in an alert which warns United States citizens about these scams, the Office of the Inspector General explained, “[Pig butchering] is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies.”²

¹ Exh. A, FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering”

² Exh. B, Office of the Inspector General Warning on Pig Butchering Scams

According to the United States Institute of Peace,

From their base in ungoverned stretches of Southeast Asia, international criminal networks are prowling the Internet, seeking to defraud victims around the world with sophisticated and psychologically devastating scams. Gangsters operating out of Myanmar, Cambodia and Laos, relying on forced labor, have spread their tentacles through Asia, Africa and Latin America and increasingly within the United States, stripping gullible prey of at least \$64 billion annually.³

Of that astounding figure, the FBI's 2023 report indicates that cryptocurrency-related fraud resulted in over \$5.6 billion in losses for United States citizens specifically, highlighting the severity and prevalence of such schemes within the confines of our own borders.⁴ The circumstances surrounding Plaintiff's case bear the distinctive hallmarks of a sophisticated "pig butchering" scheme, mirroring the insidious patterns that have come to define these elaborate cryptocurrency frauds. The intricate web of deception woven in this instance aligns precisely with the modus operandi of these notorious scams, leaving little doubt as to the nature of the malicious operation that has ensnared Plaintiff.

Plaintiff seeks leave of Court to serve limited, immediate discovery on the third-party cryptocurrency exchanges, Binance, OKX, HTX, and Crypto.com, including Know Your Customer (KYC) and Anti-Money Laundering (AML)⁵ information to help identify the names of the Defendants and their locations, as well as account details to prevent further dissipation of the assets.

³ Exh. C, United States Institute of Peace Publication on Pig Butchering Scams.

⁴ https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf

⁵ Know Your Customer information is information collected by cryptocurrency exchanges pursuant to Anti Money Laundering (AML) regulation and includes any information used to establish a user's identity. This is generally full legal name via a government-issued identification like a passport, driver's license, or other similar forms of identification.

Plaintiff served Defendants via NFT pursuant to this Court's order permitting alternative service (Doc. No. 12.) on March 28, 2025. Defendants have not answered, appeared, or otherwise communicated with Plaintiff or Plaintiff's counsel. Thus, at this stage, Plaintiff's only means to uncover the identities of the Defendants who defrauded Plaintiff of his cryptocurrency is through the cryptocurrency exchanges where those Defendants hold accounts.

III. LEGAL STANDARD

Federal Rule of Civil Procedure 26(d) generally prohibits a party from seeking discovery before the Rule 26(f) conference. However, courts may approve expedited discovery where the circumstances warrant such relief.

While the Federal Rules do not specify a standard for courts to apply when deciding to order expedited discovery, it is widely recognized that courts typically use one of two standards to determine if a party is entitled to such discovery: (1) the preliminary-injunction-style analysis established in *Notaro v. Koch*, 95 F.R.D. 403 (S.D.N.Y. 1982); or (2) the "good cause" standard.

Under the "Good Cause" standard, which is the standard generally applied within the Fifth Circuit, courts permit such discovery "where the need for expedited discovery in consideration of the administration of justice, outweighs the prejudice to the responding party." *See Yogaratnam v. Doe*, No. 1:23-CV-00393 (E.D. La. Nov. 19, 2024) (granting expedited discovery in a nearly identical cryptocurrency theft case); *Chow v. Defendant "I"*, No. 2:24-CV-00480-DJP-DPC (E.D. La. Nov. 4, 2024) (same); *Cohn v. Popescu*, No. 1:24-CV-00337, 2024 WL 4525511 (E.D. Tex. Aug. 16, 2024) (same); *Ahmed v. Doe*, No. 3:24-CV-00123-MCR-HTC (Il. N.D. Sept. 20, 2024) (granting expedited third party discovery to identify Doe defendants); *Strivelli v. Doe*, No. 22-cv-22060 2022 WL 1082638, at *2 (D.N.J. Apr. 11, 2022) (authorizing expedited discovery from cryptocurrency exchanges in crypto case and noting "the Court's review of cryptocurrency theft

cases reveals that courts often grant motions for expedited discovery to ascertain the identity of John Doe defendants”).

Additionally, a good cause analysis considers factors such as the “breadth of the discovery requests, the purpose for requesting expedited discovery, the burden on the [party] to comply with the requests and how far in advance of the typical discovery process the request was made. *BKGTH Prods., L.L.C.* at *4; *see also D.H. Griffin Wrecking Co., Inc. v. 1031 Canal Dev., L.L.C.*, No. CV 20-1051, 2020 WL 8265341, at *2 (E.D. La. Apr. 16, 2020) (quoting *BKGTH Prods., L.L.C. v. Does 1-20*, Civ. A. No. 13-CV-5310, 2013 WL 5507297 at *4 (E.D. La. Sept. 30, 2013)). Many courts have authorized expedited discovery from cryptocurrency exchanges in cryptocurrency-related fraud cases like this one.⁶ Courts are routinely affirmatively holding that any privacy interest that alleged cybercriminals have concerning the discovery of information about their identities and activities is outweighed by the need to adjudicate victims’ claims against them.⁷

IV. ARGUMENT

A. Good Cause Exists for Expedited Discovery

Here, the need for expedited discovery greatly outweighs the burden on the responding parties and is necessary to the administration of justice. Plaintiff is the victim of a typical pig

⁶ *See, e.g., Strivelli v. Doe*, No. 22-cv-22060 2022 WL 1082638, at *2 (D.N.J. Apr. 11, 2022) (authorizing expedited discovery from cryptocurrency exchanges in crypto case and noting “the Court’s review of cryptocurrency theft cases reveals that courts often grant motions for expedited discovery to ascertain the identity of John Doe defendants”); *Licht*, 2023 WL 4504585, at *4 (issuing broad authorization for expedited discovery in functionally identical crypto-fraud case and requiring that “any party served with a request for production shall produce all requested items within 72 hours of the request”); *Cohn*, 2024 WL 4525511 at *5 (authorizing expedited discovery from cryptocurrency exchanges as well as content delivery networks in an identical crypto case).

⁷ *Gaponyuk*, 2023 WL 4670043, at *4 (finding alleged cybercriminals’ privacy interests were “outweighed by the need to adjudicate the [victim’s] claims,” and holding that “privacy concerns shall not be a just cause for [a] subpoenaed non-party to withhold [] requested documents and information”).

butchering scam wherein Defendants hid their true identities to carry out their fraudulent scheme and ultimate theft of Plaintiff's cryptocurrency funds. The scam artist Defendants have vanished with only the blockchain as a trace. The cryptocurrency exchanges possess, by virtue of collected KYC and AML information, the information which will identify Defendants and also all details regarding the status of Plaintiff's funds that now sit in wallets on their respective exchanges. To date, Plaintiff has made many attempts to procure the information from the exchanges to no avail; the exchanges are largely unresponsive such that a court order is required to acquire the information from the respective exchanges. The burden on the exchanges is minimal; they have already been provided with the exact wallet addresses and they only need extract the digital account information and transmit to Plaintiff.

As to the other factors considered in a good cause analysis, the breadth of the request is reasonable. The request is narrowly drafted for the purpose of serving Defendants via traditional methods and determining the current status of Plaintiff's stolen funds. As it relates to the purpose of the request, discovery is necessary to allow this case to proceed. As discussed above, there is little effort required to comply with the request. Further, given that it is necessary to acquire the relevant identifying information to serve Defendants via traditional methods, the final factor regarding the posture of the litigation is inapplicable in this analysis.

Simply put, good cause exists for expedited discovery in this case for the following reasons:

1. The information sought is necessary to identify and serve the Doe Defendants, allowing this case to proceed.
2. There is a risk that cryptocurrency assets may be further transferred or dissipated if discovery is delayed.

3. The requested discovery is narrowly tailored and limited to information necessary to identify the Doe Defendants and to prevent the dissipation of any assets that might remain at the cryptocurrency exchanges. *See Hum. Rts. Watch v. Drug Enf't Admin.*, No. CV152573PSGJPRX, 2015 WL 13648069, at *3 (C.D. Cal. July 10, 2015) (“A party's expedited discovery requests should be ‘narrowly tailored’ so as to discover only the ‘minimum amount of information needed’ to achieve its stated purpose.”)); *see also Elargo Holdings, LLC v. Doe-68.105.146.38*, at *4. Plaintiff seeks to serve subpoenas on Binance, OKX, HTX, and Crypto.com for the following limited and specific information related to the wallet addresses associated with the alleged theft, which is This information is necessary to identify the Defendants and is proportional to the needs of the case.
 - a. Account holder's name, address, phone number, and email address.
 - b. Know Your Customer (KYC) and Anti-Money Laundering (AML) information.
 - c. Account balances and transaction history to prevent the further dissipation of Plaintiff's stolen assets.
 - d. Records of transfers to/from the relevant wallet addresses to further prevent the dissipation of Plaintiff's stolen assets.
4. The cryptocurrency exchanges, as third parties, will not be unduly burdened by the requested subpoenas.

V. CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court grant this Motion and enter an Order:

1. Authorizing Plaintiff to serve third-party subpoenas on Binance, OKX, HTX, and Crypto.com to obtain the information described above;
2. Directing the cryptocurrency exchanges to respond to the subpoenas within 14 days of service; and
3. Granting such other relief as the Court deems just and proper.

L.R. 7.1 CERTIFICATION

Defendants have concealed their identities and locations as set forth above. Accordingly, Plaintiff has been unsuccessful in locating Defendants despite diligent efforts, and, therefore, unable to confer with opposing counsel.

Dated: April 22, 2025.

Respectfully Submitted,

/s/ Reagan Charleston Thomas
Reagan Charleston Thomas, Esq.
Attorney-in-Charge
(Admitted Pro Hac Vice)
La. Bar No. 38522
**AYLSTOCK, WITKIN,
KREIS & OVERHOLTZ, PLLC**
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449
rthomas@awkolaw.com

/s/ Marshal J. Hoda
Marshal J. Hoda, Esq.
Tx. Bar No. 24110009
THE HODA LAW FIRM, PLLC
3120 Southwest Fwy
Ste. 101 PMB 51811

Houston, TX 77098
Telephone: 832-848-0036
marshal@thehodalawfirm.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on April 22, 2025, a true and correct copy of the foregoing was electronically filed with the Clerk of Court and served using the CM/ECF system. Additionally, a true and correct copy was uploaded to the Plaintiff's Service Website (<https://usdccourtservice.com/cv-04769/>).

Respectfully Submitted,

/s/ Reagan Charleston Thomas
Reagan Charleston Thomas, Esq.
Attorney-in-Charge
(Admitted Pro Hac Vice)
La. Bar No. 38522
AYLSTOCK, WITKIN,
KREIS & OVERHOLTZ, PLLC
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449
rthomas@awkolaw.com